Identifying and Balancing Privacy Responsibilities between Stakeholders

Thank you for the opportunity to comment on the National Privacy Research Strategy. As privacy researchers, we believe the creation of a national privacy research strategy is timely and will likely result in paradigm changing research. In this comment, we focus on the potential impact of governmental policy on privacy disparities between organizations and individuals.

In the current digital age, organizations must provide appropriate privacy protections while embracing technological innovations (Ernst & Young 2013), and also maintaining their competitive advantages. At the same time, individuals must be aware of how organizations are protecting their personal information. Organizations either react to privacy issues and focus on safeguards that can prevent issues for individuals and themselves, or look beyond privacy safeguards as a protection mechanism and/or instead empower customers to influence how organizations can use of their information (Price Waterhouse Coopers 2014). Two recent examples illustrate the privacy disparities between organizations and individuals.

The first example illustrates the influence that legal regulations have had on the approach Google takes toward providing privacy rights to individuals. The European Court of Justice mandated that Google provide Europeans 'the right to be forgotten' by requesting that links to web content that portrays them negatively no longer show up in search results (Tung 2014). This court order was necessary because Google refused to provide individuals with control over their own personal information in this situation. After the ruling, Google leadership did not believe this law applied to them and fought against the removal of individual search results from search queries they returned.

Google has demonstrated that being in control of the management and presentation of individual information, and providing these as part of search results, is of immense value to the organization. This indicates that they treat information as a commodity, and likely view the privacy-related legal battles as part of the cost of doing business.[1] This has resulted in Google fighting for the right to be able to continue providing these results (Tung 2014) and leaving as much information available in their search results as possible, including flagging search results

[1] For example, with revenues in excess of $60 billion in 2013, Google can pay a fine in a matter of minutes (http://my.firedoglake.com/consumerwatchdog/2013/04/03/google-may-face-more-fines-for-privacy-violations-in-europe/). Even the fine Google paid for intercepting WiFi traffic, $7 million, was paid for in one hour (http://phys.org/news/2013-03-google-fined-street-view.html).

that have had some information removed (Halliday 2014) and planning to only remove the search engine results from searches done and displayed in the European Union (Brian 2014). In this way, Google maintains the value of their collected information even when they may have to limit their public use.

The case of Google demonstrates that although there are regulations in place to provide citizens with a certain level of privacy, some organizations will find ways to minimally comply with regulations that do not align with their business strategy. In the case of Google, legal regulations are being put into place to try and provide a balance of power over information back to the individual.

Target's recent security breach provides a second example of how some organizations prioritize their own best interests over that of their customers' information privacy, often with little to no protection mechanisms available to the individual. Two circumstances distinguish this case. First, there was a security breach; second, Target failed to notify the compromised customers until after they had known for at least a week (Riley et al. 2014), in violation of the Fair Information Principle of securing customer information. Target's customers trusted them to properly handle their financial information provided during the transaction process. Target implicitly promised customers that they would provide appropriate controls on their information when accepting credit card information during the checkout process. Also, Target did not explicitly define, or give notice to customers, about what information they were collecting and storing. Target's failures illustrate how some corporations make privacy decisions inconsistent with Fair Information Principles that can actually harm customers.

These two examples are consistent with information management issues at the heart of many organizational decisions. It is recommended that information be managed with as much care as they provide to the organization's people, plant and capital (Lewis et al. 1995). As companies implement e-business solutions, the management of customer information requires further privacy considerations especially considering that these endeavors "capture, integrate and distribute data gained at the organization's website throughout the enterprise" (Pan and Lee 2003). This results in a fundamental privacy trade-off between the promise of customized goods and services and the concern for the amount of detailed information being collected to enable such customization (Awad and Krishnan 2006; Sutanto et al. 2013; Winer 2001).

Given these organizational level issues, where individuals have little to no control over their information after the organization possesses it, there also exists the question of why individuals 'freely' provide the amount of information that they do. As more companies try to make money in an environment that is increasingly relying upon individuals providing information, whether it be through social networks or location-based information on mobile devices, these issues will only continue to be magnified. While companies like Google and Facebook grew to the size that they did through providing a service in exchange for vast amounts of individual information, many more companies likewise wish to capitalize on the 'free' acquisition of individual information. While individuals may not like what companies are doing with their information, the responsibility of when to initially release that information lies with the individual. This results in three broad classes of interesting research areas that needs to be explored: 1) Policy issues targeted at organizations; 2) Sociological issues targeted toward understanding individual privacy understanding and behaviors; and, 3) Societal and economic pressures for individuals to provide personal information to participate in society. While many of these issues relate to legal and sociological research perspectives, we present how privacy-enhancing technologies will provide the means for a cross-disciplinary understanding of these privacy issues in the digital world.

Regulations and laws typically target organizations, and much care needs to be taken as they are crafted. While there is an obvious need to provide protection to the individual consumer, if regulations are overly invasive, then opportunities for economic growth and innovation may be slowed. However, if regulations are not strong enough, then the individuals will be provided with a limited increase in the amount of protection that they have. Research into the implications of different privacy regulations will help to ensure that the regulations take the right approach to balancing the protection of consumers with the ability of organizations to continue innovating and driving the economy. However, the creation of regulations requires legislators to design the correct solution in a regulatory environment that is often influenced by lobbyists. If researches can design privacy-enhancing technologies, it may be possible to relieve regulators of the need to create the perfect balance between organizations and consumers in their regulations, or at a minimum, to provide alternate technologies for enforcing regulations. Privacy has a history of self-regulation through the implementation of privacy seals (LaRose and Rifon 2007). Although, privacy seals were not a perfect implementation, they did enable

organizations to avoid legislated privacy-related changes. Similarly, privacy-enhancing technologies could provide an avenue for organizations to participate in some forms of self-regulation in an attempt to avoid the need for regulations. Doing so with the help of well-founded research would aid in ensuring that the interests of individuals were considered as requirement in the design of these solutions.

Research that explores individuals' information sharing intentions and other privacy sharing behaviors has been conducted for a number of years. However, there is limited research that explains the actual information sharing practices of individuals in an era where people utilize mobile devices that are in essence a computer in their pocket. The always-available access to the Internet through mobile technologies and the ability to share location-based information forces individuals to make information sharing decisions on a regular basis. Does this regularity of privacy sharing information impact the likelihood that people will mistakenly share information when they had no intention to? As the influence of this always on nature to information availability is understood, then perhaps privacy-enhancing technologies can be put in place to help individuals understand and track the information they are sharing. This approach to providing solutions would allow individuals to have a better understanding of how they share their information, and as a result a greater ability to take more control over who they share it with and for what purposes. This insight may also help in the proper development of an accepted standard for organizations to agree upon as to how and when information is being collected. Such a standard could provide a common platform for collecting and storing individuals' information consistently across all types of technologies.

The *modus operandi* of making money on the Web is through the collection of consumer information. With increasing frequency, individuals cannot access information online without providing their personal information. This creates an interesting problem for users of this service as their choice becomes to use the Web and give out their personal information, or disconnect completely and miss out on information opportunities. An interesting area of research would be to explore viable profit mechanisms that people would still use that do not require the sacrificing of their personal information. Is there a price people would pay for a guaranteed right to privacy? Could a privacy-enhancing technology be designed that individuals would be willing to pay for because it provides them with control of their private information? Is there another way to create a privacy-enhancing technology that would be profitable for companies to monetize by

providing content online without exploiting individual information and without costing or risking anything for the individual to participate? As these research questions are addressed, the future of the Internet can be shaped in a way that will be a win-win for the individual and the organization.

In conclusion, the current state of the Internet raises an interesting question of whose responsibility is privacy protection. Does it rest solely with the individual, organizations collecting the information, or through some balance that is regulated by the government? Is it possible for privacy-enhancing technologies to be utilized in a way that provides this balance so that government regulation is not necessary?

As research explores the issue of privacy in the digitally connected world, any insight into these concerns will only make it a better service that will continue to grow our economy into the future.

References

Awad, N. F., and Krishnan, M. S. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization," *MIS Quarterly* (30:1) 2006, pp. 13-28.

Brian, M. 2014. "What You Need to Know About the 'Right to Be Forgotten' on Google." from http://www.engadget.com/2014/06/02/right-to-be-forgotten-explainer/.

Ernst & Young. 2013. "Privacy Trends 2013: The Uphill Climb Continues." Retrieved June 3, 2014, from http://www.ey.com/Publication/vwLUAssets/Privacy_trends_2013_-_The_uphill_climb_continues/$FILE/Privacy%20trends%202013%20-%20The%20uphill%20climb%20continues.pdf.

Halliday, J. 2014. "Google Search Results May Indicate 'Right to Be Forgotten' Censorship." from http://www.theguardian.com/technology/2014/jun/08/google-search-results-indicate-right-to-be-forgotten-censorship.

LaRose, R., and Rifon, N. J. "Promoting I-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior," *The Journal of Consumer Affairs* (41:1) 2007, pp. 127-149.

Lewis, B. R., Snyder, C. A., and Rainer Jr, R. K. "An Empirical Assessment of the Information Resource Management Construct," *Journal of Management Information Systems* (12:1) 1995, pp. 199-223.

Pan, S. L., and Lee, J. "Using E-Crm for a Unified View of the Customer," *Communications of the ACM* (46:4) 2003, pp. 95-99.

Price Waterhouse Coopers. 2014. "10 Minutes on Data Privacy." Retrieved June 3, 2014, from http://www.pwc.com/en_US/us/10minutes/assets/pwc-data-privacy.pdf.

Riley, M., Elgin, B., Lawrence, D., and Matlack, C. 2014. "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It." Retrieved June 10, 2014, from

http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

Sutanto, J., Palme, E., Tan, C. H., and Phang, C. W. "Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users," *MIS Quarterly* (37:4) 2013, pp. 1141-1164.

Tung, L. 2014. "Google Loses 'Right to Be Forgotten' Fight in Europe's Top Court." Retrieved June 10, 2014, from http://www.zdnet.com/google-loses-right-to-be-forgotten-fight-in-europes-top-court-7000029383/.

Winer, R. S. "A Framework for Customer Relationship Management," *California Management Review* (43:4) 2001, pp. 89-105.